GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: REVISIÓN BIBLIOGRÁFICA

Information security management: A bibliographic review

Leidy-Johanna Cárdenas-Solano, Hugo Martínez-Ardila y Luis-Eduardo Becerra-Ardila

Leidy-Johanna Cárdenas-Solano es ingeniera industrial por la *Universidad Industrial de Santander* (*UIS*), Colombia y candidata a MSc. en ingeniería industrial (*UIS*). Investigadora del *Center for Technology and Innovation Management Research* (*Innotec*). Docente del grupo de investigación en gestión industrial y administrativa de la *Universidad Manuela Beltrán* (*UMB*). Sus intereses se centran en la gestión del conocimiento, gestión de seguridad de la información, aseguramiento del conocimiento, vigilancia tecnológica, patentes, e incubadoras de empresas de base tecnológica
http://orcid.org/0000-0001-5471-7160

leidy.cardenas2@correo.uis.edu.co

Hugo Martínez-Ardila es ingeniero electrónico por la *Universidad Industrial de Santander* (*UIS*), Colombia, MSc en ingeniería (*UIS*), PhD en ingeniería área gestión y desarrollo tecnológico (*UIS*), investigador del *Center for Technology and Innovation Management Research* (*Innotec*). Director de la *Oficina de Transferencia de Resultados de Investigación Estratégica de Oriente* (*Colciencias*), *Cámara de Comercio de Bucaramanga*. Sus intereses se centran en innovación abierta, gestión de la innovación y redes de innovación.
http://orcid.org/0000-0001-6893-0819

hugom@saber.uis.edu.co

Luis-Eduardo Becerra-Ardila es ingeniero industrial por la *Universidad Industrial de Santander* (*UIS*), Colombia, MSc en administración del *Instituto Tecnológico de Estudios Superiores de Monterrey* y estudiante de doctorado en ingeniería en la *UIS*. Es profesor titular de la *Escuela de Estudios Industriales y Empresariales* de la *UIS*, y director del grupo de investigación *Center for Technology and Innovation Management Research* (*Innotec*). Sus intereses se centran en la gestión tecnológica, ciudades inteligentes, gestión del conocimiento, gestión financiera e incubadoras de empresas.
http://orcid.org/0000-0002-2596-3853

lbecerra@uis.edu.co

Universidad Industrial de Santander
Carrera 27, calle 9, Ciudad Universitaria. 680006 Bucaramanga, Colombia

Resumen

Desde 1969, cuando Peter Drucker pronosticó el surgimiento de la "sociedad del conocimiento", el capital intelectual de las organizaciones ha tomado más importancia en el mundo empresarial, por ser uno de los indicadores para valorar una compañía. De ahí la necesidad de protegerlo, labor que puede ser realizada a través de la gestión de la seguridad de la información. El objetivo de este trabajo es consolidar el estado del arte sobre el tema "information security" para la ventana de tiempo 2001-2015. La revisión bibliográfica se realizó en tres etapas: a) Revisión de información no estructurada, b) Análisis bibliométrico y c) Análisis, organización y síntesis del contenido. Como resultado se extrajo un amplio marco de trabajo multi-dimensional en el que se relaciona gestión del conocimiento, gestión de riesgos, incidentes de seguridad, sistemas de información y redes, recursos humanos, aspectos económicos, gobernanza, políticas, y buenas prácticas. De lo anterior se concluye que en la bibliografía analizada existen espacios para futuras líneas de investigación relacionadas.

Palabras clave

Gestión del conocimiento; Seguridad de la información; Marcos de trabajo; Buenas prácticas; Cultura de la seguridad de la información; Gestión de la seguridad de la información; Revisión bibliográfica; Estado del arte.

Artículo recibido el 09-06-2016
Aceptación definitiva: 24-10-2016

Abstract

Since 1969, when Peter Drucker forecasted the emergence of the "knowledge society", the intellectual capital of organizations has become more important in the business world; for this reason, it needs to be protected. Such a task can be accomplished through information security. This paper is a review of the topic "information security" for the period 2001-2015 and, on this basis, provides the key to designing a management model of information security factors. The bibliographic review was conducted in three stages: a) review of unstructured information, b) bibliometric analysis, and c) content analysis, organization, and synthesis. As a result, a multi-dimensional framework was obtained, where relations among knowledge management, risk management, security incidents, information systems, and networks, human resources, economic aspects, governance of information security, policies, and good practices were studied. It is concluded that there are gaps for future research.

Keywords

Knowledge management; Information security; Frameworks; Best practices; Information security culture; Information security management; Literature review; Bibliography; State of the art.

Cárdenas-Solano, Leidy-Johanna; **Martínez-Ardila, Hugo**; **Becerra-Ardila, Luis-Eduardo** (2016). "Gestión de seguridad de la información: revisión bibliográfica". *El profesional de la información*, v. 25, n. 6, pp. 931-948.

https://doi.org/10.3145/epi.2016.nov.10

1. Introducción

Hace unos 30 años, académicos como **Drucker** (1988), **Porter** y **Millar** (1985), fueron los primeros en reconocer la existencia de una "revolución de la información" con efectos significativos en todos los aspectos de la vida organizacional (**Zammuto** *et al.*, 2007). La experiencia ha demostrado que una buena gestión de la información, no sólo puede mejorar el desempeño organizacional (**Brynjolfsson**; **Hitt**, 1996; **Sircar**; **Choi**, 2009, citado por **Doherty**; **Anastasakis**; **Fulford**, 2009; **Ward**; **Peppard**, 2002, citado por **Doherty**; **Anastasakis**; **Fulford**, 2009), sino también transformar radicalmente los procesos, estructura y cultura de la organización (**Doherty**; **King**; **Al-Mushayt**, 2003; **Markus**, 2004).

> La seguridad de la información ha evolucionado desde la seguridad física orientada a la protección de ordenadores a concentrarse en políticas, procedimientos y controles basados en las personas

La información ha sido vista a menudo como la "sangre" de la organización (**Halliday**; **Badenhorst**; **Von-Solms**, 1996; **Gerber**; **Von-Solms**, 2005; **Peppard**, 2007). Si el flujo de información es continuo, los procesos se ejecutarán de manera óptima; pero si es restringido o seriamente perturbado, la organización se puede deteriorar o incluso morir, lo cual se convierte en un riesgo de seguridad de la información. Acerca de cómo prevenir estos riesgos, **Mitnick**, **Simon** y **Wozniak** (2003, p. 79) hicieron la siguiente afirmación:

> "Nunca se confíe de los mecanismos de seguridad en la Red para proteger su información. Revise su punto más vulnerable. En la mayoría de los casos descubrirá que éste se encuentra en las personas".

La seguridad de la información ha evolucionado desde la seguridad física orientada a la protección de ordenadores y dispositivos de almacenamiento de información, pasando por la seguridad de sistemas y redes de tecnologías de información, a concentrarse en la gestión de alto nivel mediante políticas, procedimientos y controles basados en las personas (**Nnolim**, 2007). Este autor sostuvo también que, a pesar de la evolución exponencial y relevancia del tema, no existen directrices que proporcionen la base teórica necesaria para un marco y una metodología de gestión de la seguridad. Algunos autores como **Hong** *et al.* (2003) sugieren que la ausencia de un marco y una metodología ha contribuido a la falta de teoría científica en este tema.

En este contexto, el propósito de este trabajo es comprender la evolución de la gestión de la seguridad de la información (GSI) en la bibliografía. Esta investigación no se ha delimitado a un cierto nivel (es decir, macro o micro); los términos de búsqueda se mantienen amplios para no limitar la investigación a un área determinada dentro del tema.

> No existen directrices que proporcionen la base teórica necesaria para un marco y una metodología de gestión de la seguridad

2. Metodología

Una revisión sistemática requiere de una secuencia de localizar, analizar, ordenar, contar y evaluar bibliografía de fuentes definidas a través de un período de tiempo. Sus ventajas son que el proceso es replicable, científico y transparente (**Tranfield**; **Denyer**; **Smart**, 2003). Este trabajo propone revisar los conceptos asociados a la GSI en las organizaciones, con base en un protocolo que permitió definir anticipadamente los criterios y parámetros específicos del proceso de búsqueda y análisis de la información. En él se especificó el proceso que se seguiría durante la búsqueda, los filtros a utilizar para la selección de la información, y el flujo que esta seguiría hasta ser estructurada adecuadamente. Lo anterior se resume en tres grandes fases:

- elección de la fuente de información y selección de los datos de la muestra;
- transformación de los datos mediante el uso de técnicas bibliométricas;
- reporte de los resultados.

La revisión de bibliografía se realizó mediante métodos mixtos, es decir, análisis de contenido[1] y análisis estadístico (**Lu** *et al.*, 2014), por lo cual no sólo se identificaron tendencias de publicación, principales autores y revistas, sino que además se gestionaron, codificaron y analizaron los diversos elementos o datos de los documentos con el apoyo del software de análisis cualitativo de datos *Maxqda*, que permitió analizar datos estructurados. El reporte de la revisión sistemática fue construido y actualizado en el transcurso de la investigación.

La revisión partió de una consulta exploratoria, mediante la cual se identificó como término equivalente a seguridad de la información la expresión *information security*. Se seleccionó la base de datos *Social Sciences Citation Index* (*SSCI*) de la *Web of Science*, teniendo en cuenta que es una referencia internacional por su contenido de artículos de calidad y solapo de cerca del 80% con la base de datos *Scopus* (**Martínez-Acevedo** *et al.*, 2013). Además comprende revistas especializadas de calidad en ciencias sociales y es una de las más importantes e influyentes del mundo (**Lim**, 2004; **Testa**, 2001).

La ecuación de búsqueda (se utilizó en el campo Topic) fue:

TS: ("information security")

Esta ecuación tenía por objetivo ser amplia y tener la máxima cobertura posible, sin dejar de tener un tamaño de los resultados manejable, por lo cual se evitó el uso de operadores lógicos, cadenas de búsqueda y restricciones en áreas específicas de seguridad con el fin de tener información completa para los análisis bibliométricos y cualitativos posteriores. Se consultó para publicaciones indexadas entre el 1 de enero de 2001 y el 30 de octubre de 2015 (fecha de última actualización de los datos).

Como resultado de la búsqueda se identificaron 1.770 documentos científicos entre artículos, revisiones, actas, material editorial, capítulos de libro, resúmenes de reunión, revisiones de libro, noticias, cartas, correcciones, impresiones, revisiones de software y bibliografías. De ellos, los artículos eran 1.227, y se exportaron de la plataforma en formato *tab delimited* (*MAC*) para la configuración de una base de datos con las etiquetas de autores, título, resumen, revista, palabras clave asignadas por el autor, institución, año de publicación y área de investigación y aplicación. Posteriormente, mediante la lectura de los títulos se excluyeron 239 artículos considerados irrelevantes puesto que incluían palabras relacionadas con construcción tales como: concreto, edificio, puente, construcción, estructura, etc., quedando un total de 988 artículos científicos.

Se realizó el examen de los títulos de los artículos basados en investigación teórica y empírica, referentes a:

- buenas prácticas en seguridad de la información;
- marcos de trabajo o metodologías para la GSI;
- políticas y controles de seguridad de la información para la gestión de riesgos desde la academia.

No se profundizó en bibliografía referente a seguridad de infraestructura tecnológica o controles técnicos de seguridad de información.

El principal foco de esta revisión fue formular un marco de referencia acerca de la gestión de seguridad de la información (GSI) en las organizaciones, y responder a la pregunta de investigación ¿cómo deben los profesionales de la seguridad de información organizar y priorizar sus esfuerzos con el fin de construir y mantener un programa de seguridad de la información con base en un protocolo, marco de referencia o marco de trabajo que permita definir anticipadamente los criterios y parámetros mínimos del programa de seguridad?

Considerando los análisis bibliométricos realizados a los 988 artículos obtenidos mediante el software de minería de datos *Vantage point*, se determinó leer los documentos completos que se obtuvieran al restringir la búsqueda al área de la administración (*management*) y ciencias afines de acuerdo con las categorías que asigna *WoS*. Además, por sugerencia de expertos y dada la necesidad de analizar la temática de seguridad de la información sobre temas de gestión, se utilizó una nueva ecuación obteniendo 26 documentos adicionales:

Topic=("information security management")

De forma semejante se realizó otra búsqueda con esta misma ecuación, en el campo Título, pero no se obtuvieron resultados significativamente diferentes.

Por último, sumado a todo lo anterior, se incluyeron otros artículos encontrados a través del método bola de nieve (**Dolan** *et al.*, 2005) (en inglés *pearl growing*), que consiste en descubrir otros documentos de interés mediante la revisión de la bibliografía citada en los documentos iniciales. Como consecuencia, se encontraron documentos de años anteriores a 2001 en otras bases de datos científicas a las que se tiene suscripción (*Emerald*, *EbscoHost*, *ScienceDirect*, *Scopus*, *ProQuest*, y *SpringerLink*), y fue posible identificar a Rossouw Von-Solms como autor relevante con un índice h de 34 y 3.928 citas, con lo que se incluyeron 16 documentos más.

Finalmente, se efectuó un segundo filtro por el contenido y tema tratado en el resumen. Se analizaron los documentos completos de 121 publicaciones y a partir de las palabras clave sugeridas por los autores, se organizaron en nueve categorías que dieron origen a un marco de trabajo (*framework*) como referencia para abordar la GSI (tabla 1). Estas categorías se construyeron tras reuniones iniciales no estructuradas del equipo de investigación tipo tormenta de ideas (*brain storming*) y el estudio de documentos alusivos a la seguridad de la información, entre los que se encuentran:

- el libro *Information security* de **Layton** (2007);
- normas de referencia o metodologías para valoración de riesgos, como *Octave* (*CERT*, s.f.), *Magerit*, *ISO/IEC 27002:2005* e *ISO/IEC 27002:2013*;
- guías de seguridad de la información, como la proporcionada por *NIST*[2];
- estudios institucionales y de organismos internacionales;
- revisión del *Aduna cluster map* obtenido a través de *Van-*

tange point (figura 1), el cual representa en cada color las categorías. Éstas son aquellas palabras clave de los autores más importantes en la publicación global del área de seguridad de la información, mostrando con círculos amarillos la cantidad de artículos, ya sea que discutan acerca de un solo tema a la vez o que hablen sobre dos o más temas (las cantidades de dos o más temas se muestran en las intersecciones de estos colores con un círculo amarillo dispuesto en el enlace).

Las limitaciones de esta investigación surgen de la imposibilidad de realizar una triangulación de investigadores que permita reducir los sesgos de utilizar un único equipo de investigación para recolectar, analizar y asociar las palabras claves sugeridas por los autores de los artículos a las categorías definidas (**Okuda-Benavides; Gómez Restrepo**, 2005), con la intención de dar un mayor nivel de validez al marco de referencia concluido. Sin embargo, este trabajo se propone como punto de partida para futuras investigaciones que contemplen la profundización en cada una de las categorías organizativas propuestas y el estudio en diversos contextos organizativos de otros marcos de trabajo.

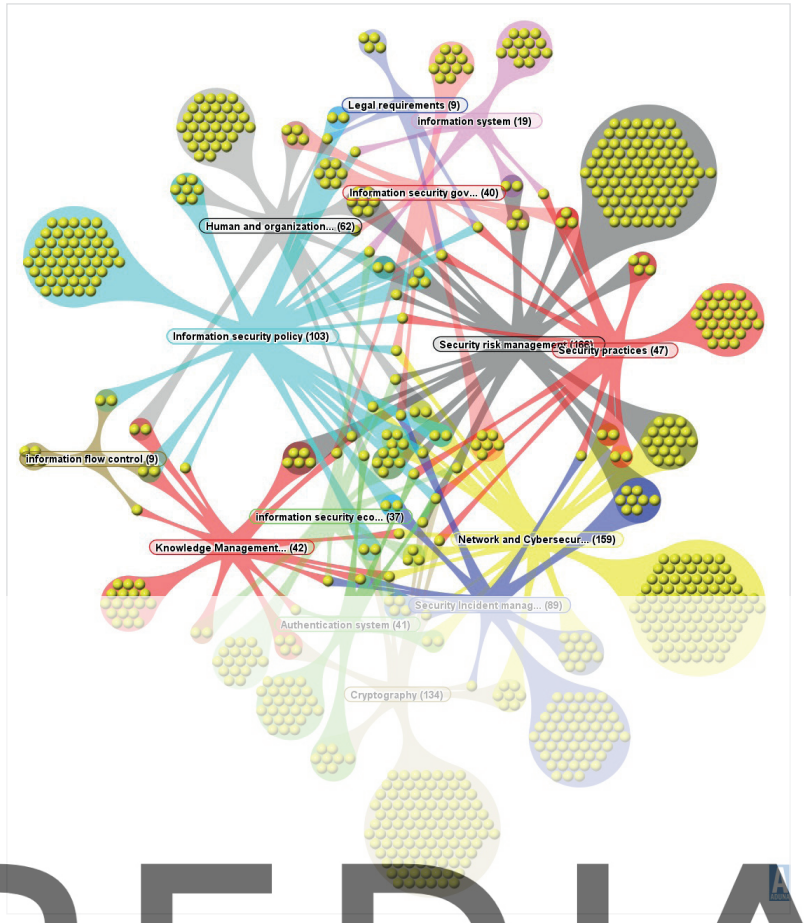

Figura 1. *Aduna cluster map* de las relaciones estrechas entre palabras clave. Se ha usado *Vantange point*. Noviembre de 2015.

3. Resultados

De acuerdo con la bibliografía evaluada, la seguridad de la información es un tema en rápido crecimiento. El número de artículos encontrados es de 1.770, con un promedio de citas por año de 691,27. En 2014 el número de publicaciones ya se había duplicado con respecto a 2001, sumado a que en el informe de citas para 2001 sólo se registra una referencia citada, correspondiente al artículo de **Dhillon** (2001), el cual tiene a la fecha 66 citas posteriores. Lo anterior permite afirmar que es un tema que aún no llega a su etapa de madurez, y se refleja en los incrementos porcentuales positivos año a año, que dan la oportunidad de explorar el tema y enriquecerlo en el futuro (figura 2).

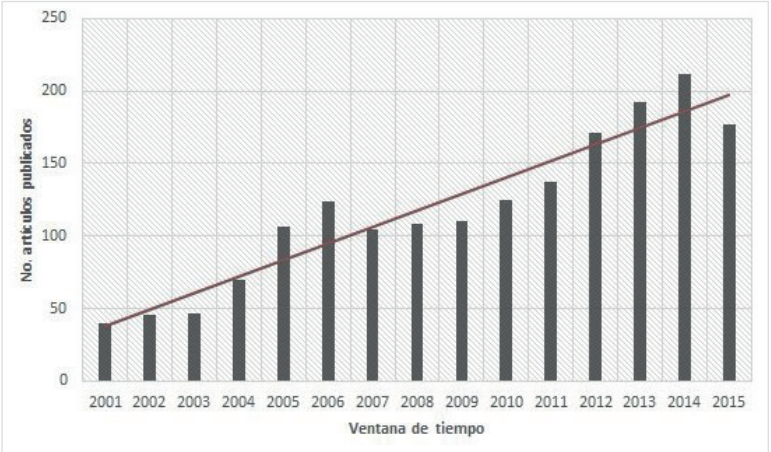

Figura 2. Tendencia anual de publicación de artículos sobre "*information security*". Datos obtenidos de la *Web of Science*. Octubre de 2015.

Se analizó el número de publicaciones por año mediante *Vantange point* según las palabras clave sugeridas por los autores (figura 3), y se esperaría que:

- el tema "*information security system*" alcanzó su nivel de madurez en 2013, y luego empieza un declive, pasando de 81 publicaciones en 2013 a 56 en 2015;
- el tema "*network and cybersecurity systems*" a partir del año 2012 empieza a ser más abordado, y pasa de 20 publicaciones en 2012 a 28 en 2015;
- el tema "*data security*" gana espacio en la comunidad académica y en el interés de los investigadores, pasando de 19 publicaciones en 2013 a 25 en 2015.

La revisión sistemática de artículos publicados entre 2000 y 2014 realizada por **Rahim *et al.*** (2015) indica que ninguna investigación anterior se llevó a cabo para evaluar el conocimiento de seguridad cibernética. También se encontró que pocos estudios se han centrado en la protección de la información personal. Es coherente que la ciberseguridad sea un tema en auge y contenga los mayores retos tanto para el sector empresarial como el científico en los próximos años. Esto se refleja en la preocupación con respecto a las violaciones de seguridad cibernética que ha llevado a la necesidad de proteger los me-

dios de información y almacenamiento (**Dlamini**; **Eloff**; **Eloff**, 2009).

Uno de estos medios es la computación en la nube o CC (en inglés, *cloud computing*), descrita por el *National Institute of Standards and Technology* (*NIST*) de los EUA como un modelo que permite el acceso bajo demanda a una serie de recursos informáticos compartidos (redes, servidores, sistemas de almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y puestos en funcionamiento con un mínimo esfuerzo de gestión e interacción con el proveedor de servicios (**Mell**; **Grance**, 2011). Una de las principales razones por las que el crecimiento de la CC ha sido lento son los incidentes de seguridad, que han dado lugar a publicaciones sobre este tema (**Modi** *et al.*, 2013). Ésta parece ser un área prometedora para la investigación y evaluación de la seguridad puesto que, a pesar de la investigación que se ha llevado a cabo en seguridad CC, según **Cruz-Zapata**, **Fernández-Alemán** y **Toval** (2015), es necesario evaluar el estado actual de la investigación para proporcionar a los profesionales la evidencia que les permitirá centrarse en su desarrollo posterior.

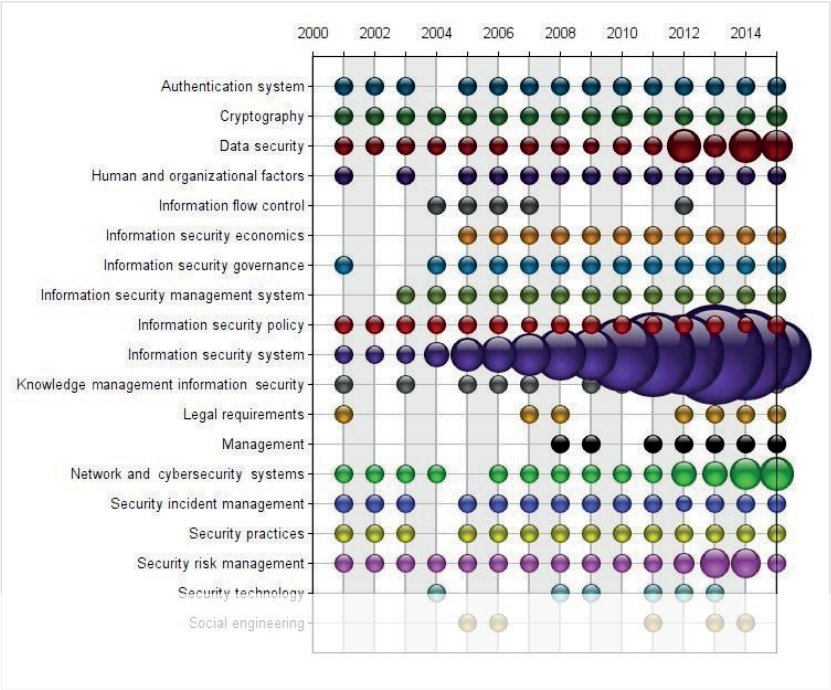

Figura 3. Tendencia de publicación de las *keywords* o descriptores de la búsqueda "*information security*". Se ha usado el programa *Vantange point*. Noviembre de 2015.

> Según el análisis de la bibliografía, la seguridad de la información es un tema en rápido crecimiento

El aumento de publicaciones sobre *data security* se debe a que los métodos de protección utilizados deben ser actualizados en línea con los nuevos avances tecnológicos para hacer frente a las amenazas a la seguridad cibernética cada vez más sofisticados procedentes de fuentes no previstas en internet (**Choo**, 2011; **Dlamini**; **Eloff**; **Eloff**, 2009). La naturaleza de las amenazas informáticas de hoy es más sofisticada y sin precedentes en términos de alcance, habilidad, frecuencia, y capacidad. De realizarse podrían dar lugar a graves pérdidas económicas (**Albrechtsen**, 2007).

Actualmente el principal factor que contribuye a los cambios en las amenazas informáticas es la creciente población mundial que utiliza internet. A junio de 2014 más de tres mil millones de personas en todo el mundo estaban usando internet, y la mayoría de los usuarios eran del continente asiático (**Sanou**, 2014). Lo anterior se suma a las nuevas aplicaciones que contribuyen al aumento de uso de internet. El intercambio de información, la banca online, las compras, así como la comunicación interactiva y la socialización a través de la Web (**Leiner** *et al.*, 1997), invitan a muchos a unirse a internet, donde la mayoría son usuarios de entre 12 y 19 años de edad. Los jóvenes son frecuentemente categorizados como los usuarios más activos de internet, con un alto uso de dispositivos inteligentes (**Atkinson**; **Furnell**; **Phippen**, 2009; **Cole** *et al.*, 2013).

El tema de la seguridad de los datos, como se observa en el análisis bibliométrico, se asocia en gran parte al creciente uso de internet. Uno de los riesgos es la invasión silenciosa de la privacidad individual que se dirige específicamente a la obtención de los datos personales de los individuos por medios ilegales (**Aimeur**; **Schonfeld**, 2011; **Loibl**, 2005; **Broadhurst**; **Chang**, 2013). Todo esto permite plantear otros retos fuera del alcance de esta investigación, que son oportunidades para futuras investigaciones. Uno de ellos es la eficacia de los programas de sensibilización de seguridad cibernética para los más jóvenes. El primer desafío es determinar la aceptación y la comprensión del concepto de seguridad y promover una cultura de seguridad (**Kruger**; **Kearney**, 2006; **Rantos**; **Fysarakis**; **Manifavas**, 2012), teniendo en cuenta que un problema que contribuye a este factor es el exceso de confianza de los jóvenes en la seguridad de sus ordenadores personales y dispositivos móviles, lo que puede conducir a no adoptar las medidas necesarias (**Furnell**, 2008). La actitud displicente hacia la seguridad hace que sean el eslabón más débil de la cadena (**Gross**; **Rosson**, 2007) ya que a menudo son ignorantes e ingenuos acerca de estos problemas (**Furnell**; **Thomson**, 2009).

> El aumento de publicaciones sobre *data security* se debe a que los métodos de protección utilizados deben ser actualizados en línea con los nuevos avances tecnológicos

Otro de los resultados que llamó la atención fue la reducción en un 45,8% del número de publicaciones sobre el tema "*security risk management*" en 2015 frente a las 24 publicaciones realizadas en 2014. Se infiere que puede estar contrapesado por el aumento en los estudios focalizados

en ciberseguridad debido a la creciente dependencia de la tecnología y por tanto la necesidad de enfocar esfuerzos para mitigar el incremento de amenazas en los sistemas interconectados y las redes (**Broadhurst**; **Chang**, 2013). Según **Sen** y **Borle** (2015) los incidentes de violación de datos se van intensificando, y han dado lugar a consecuencias financieras y legales severas para las organizaciones afectadas. Según explican estos autores, es posible que las inversiones en seguridad de TI no están siendo utilizadas correctamente en cuanto a seguridad de datos. A ello hay que añadir la necesidad de generar una cultura de protección de datos e información en las organizaciones donde se aborde correctamente la confidencialidad, la sensibilidad y la privacidad de la información, teniendo como objetivo reducir el riesgo que la conducta humana significa para la protección de la información (**Da-Veiga**; **Martins**, 2015).

Posteriormente a los análisis bibliométricos, y una vez identificados los artículos considerados relevantes, se analizaron y se elaboró el marco de referencia para responder a la pregunta de investigación: ¿Cómo se construye y desarrolla el proceso de GSI en las organizaciones de los entornos dinámicos para la obtención de ventajas competitivas sostenibles? Como principal resultado de esta revisión de bibliografía, se agruparon las temáticas tratadas en las publicaciones en 9 categorías relacionadas entre sí como se muestra en la tabla 1, con el fin de entender la estructura de conocimiento de las investigaciones en "*information security*", sus patrones y tendencias asociadas.

Entiéndase por marco de trabajo o *framework*, según el diccionario *Oxford*, una estructura básica que subyace a un sistema, un concepto o texto. En términos más prácticos,

Tabla 1. Categorías para formular un marco de trabajo de seguridad de la información

Buenas prácticas	Políticas	Gestión de riesgos	Recursos humanos	Gestión del conocimiento	Gobernanza	Sistemas de información y redes	Economía	Incidentes de seguridad
Balanced scorecard	*Information security policies*	*Asset classification*	*Awareness*	*Customer capital*	*Corporate governance*	*Cloud computing*	*Cost of security*	*Computer crime*
Best practices	*Information security policy*	*Asset identification*	*Behavioral issues of information security*	*Human capital*	*Evaluation model*	*Computer networks*	*Cost sharing*	*Data security*
BS 7799	*Internet use policy*	*Business impact analysis*	*Behavioral operations management*	*Intellectual assets*	*Framework*	*Hacker learning*	*Economics of IS*	*Disclosures*
Business practice	*IS security policies*	*Business information risk*	*Behaviour*	*Knowledge*	*Governance*	*ICT security tools*	*Experimental economics*	*Downtime loss*
Certification	*National information security policy*	*Controls*	*Corporate culture*	*Knowledge creation*	*Information security governance*	*ICT*	*Information security economics*	*Event studies*
Compliance	*Optimal policy*	*Counter measures*	*Employee perspectives*	*Knowledge management*	*Information technology governance*	*Internet and communication technologies*	*Market value*	*Information leakage*
Conformity assessment procedure	*Policy*	*Information assets*	*Employees' compliance with security policies*	*Knowledge management capability*	*IT governance*	*Information systems*	*Optimal security investment*	*Insider trading*
Guidelines	*Policy content*	*Information security risk*	*End-user security*	*Knowledge security*	*Management frameworks*	*Information systems outsourcing*	*Technology investment*	*Missing data*
Information security certification	*Power and politics*	*Information security risk analysis*	*Information security awareness*	*Knowledge sharing*	*Management levels*	*Information systems security*	*Transaction cost economics*	*Nonmalicious security violation*
Information security compliance	*Security policy*	*Information security risk management*	*Information security culture*	*Knowledge transfer*	*Reference model*	*Information systems security management*	*Business administration/ economics*	*Organizational effectiveness*
Information security management system	*Security policy adoption*	*Information security threats*	*Information security culture*	*Practice perspective of knowledge*	*Organization*	*Information systems services*		*Security breaches*
Information security requirements	*Security policy implementation*	*Information security vulnerabilities*	*IS security training*	*Structural perspective of knowledge*	*Business process analysis*	*Information technology capabilities*		*Security shocks*
Information systems security standards	*Technology policy*	*Information systems risk*	*Online protection behaviour*	*Structure capital*		*Information technology security*		

puede considerarse como una aplicación genérica, incompleta y configurable a la que se pueden añadir piezas adicionales para construir una aplicación concreta (**Gutiérrez**, s.f.). En este sentido, un *framework* también puede ser visto como un estándar que, tomado como base o referencia, es útil para enfrentar y resolver nuevos problemas de índole similar.

Por su parte, un marco de seguridad de la información es una serie de procesos documentados que a menudo se personalizan para resolver problemas específicos de seguridad de la información, al igual que los planos de construcción pueden personalizarse para satisfacer sus especificaciones requeridas y uso. Hay marcos que fueron elaborados para industrias específicas, así como diferentes objetivos de cumplimiento normativo. También vienen en diferentes grados de complejidad y escala. Sin embargo, se encuentra que hay una gran cantidad de superposiciones en los conceptos generales de seguridad, ya que cada uno evoluciona (**Granneman**, 2013).

En este *framework* (figura 4), el elemento de mayor nivel jerárquico es la gobernanza de seguridad de la información, donde se toman las decisiones de carácter estratégico que afectan directamente el desarrollo de políticas. Normalmente existe una política general de seguridad de la información, y a partir de ella se pueden originar políticas específicas para distintas áreas de la organización. En la política también se establecen lineamientos sobre cómo, cuándo y quién lleva a cabo la evaluación y tratamiento de riesgos, actividades que constituyen la gestión de riesgos. Esta última es alimentada por los incidentes de seguridad que brindan alertas sobre riesgos no identificados o no controlados.

Como base de todas las actividades realizadas, se encuentran siempre los estándares o guías de buenas prácticas,

> Un marco de seguridad de la información es una serie de procesos documentados que a menudo se personalizan para resolver problemas específicos de seguridad de la información

que permiten conocer los requisitos mínimos para gestionar la seguridad de la información.

Por último, como tema transversal se encuentra la gestión del conocimiento, ya que cualquier esfuerzo realizado en la organización se convierte en conocimiento y experiencia que deben ser apropiados por los individuos. Asimismo, no sólo la información debe ser protegida sino también el conocimiento existente en las personas; es allí donde surgen nuevos riesgos que deben evaluarse y tratarse.

3.1. Gestión del conocimiento

Según una definición propuesta por **Wallace** (2000), la gestión del conocimiento permite habilitar personas, equipos y organizaciones completas en la creación, compartición y aplicación del conocimiento, colectiva y sistemáticamente, para mejorar la consecución de los objetivos de negocio. El

Figura 4. Marco de trabajo de seguridad de la información.

interés por este campo sigue creciendo, aunque son escasos los estudios sobre cómo proteger los activos basados en conocimiento (**Desouza**; **Vanapalli**, 2005). Por tanto, existe un gran interés en el diseño de marcos de trabajo de GSI (**Nnolim**, 2007) que proporcionen una guía en la protección de la información y conocimiento generado, gestionado y transferido en las organizaciones.

3.2. Gestión de riesgos

Según **Zhou** *et al.* (2010), las cinco metas tradicionales de la gestión de riesgos son:

- logro de una seguridad adecuada de disponibilidad
- confidencialidad
- integridad de datos
- control de acceso
- auditoría.

Gerber y **Von Solms** (2005) proponen adoptar un enfoque alternativo al análisis de riesgos tradicional, en el cual se analicen no solamente los riesgos de los activos tangibles, sino también los riesgos de los intangibles como la información.

Lategan y **Von Solms** (2006) enfatizan que las empresas deben asegurar que los riesgos sean gestionados holísticamente y que la terminología y prácticas de riesgo relacionadas con TICs estén congruentemente alineadas con la terminología y prácticas de la empresa. Hay tres fuentes principales de riesgos de información:

- riesgos asociados con los fenómenos naturales;
- riesgos de carácter técnico que resultan de la amplia dependencia de toda la organización de la tecnología;
- riesgos potenciales derivados de los humanos, que pueden afectar la información organizativa o empresarial (**Posthumus**; **Von-Solms**, 2004).

De acuerdo con **Layton** (2007):

- un riesgo está constituido por la probabilidad, impacto y consecuencia de eventos negativos que la organización debe considerar como parte de sus operaciones;
- una vulnerabilidad consiste en un defecto o debilidad en un sistema de información, procedimiento asociado, o control existente que tiene el potencial de ser ejercido (accidental o intencionalmente) y resultar en un incumplimiento o violación de la política de seguridad de la información. Según **Wang** *et al.* (2012) una vulnerabilidad se puede aprovechar para atacar el activo de información;
- la amenaza se refiere a un posible peligro o atacante que aprovecha las debilidades (vulnerabilidades del sistema) (**Whitman**, 2004).

En la figura 5 se observan las múltiples relaciones existentes entre los conceptos anteriores.

En este sentido, como uno de los primeros pasos en la implantación de un protocolo de seguridad de la información, se debe llevar a cabo una evaluación del riesgo (*risk assessment*), que consiste en identificar los riesgos de seguridad de un sistema y determinar su probabilidad de ocurrencia, su impacto, y los mecanismos que mitiguen ese impacto (**Syalim**; **Hori**; **Sakurai**, 2009).

Según la *US General Accounting Office*, la mayoría de las metodologías de evaluación de riesgos utilizadas incluyen los siguientes elementos básicos:

- identificación de las amenazas;
- estimación de la probabilidad de que dichas amenazas ocurran;
- identificación y valoración de los activos que podrían estar en riesgo;
- cuantificación del impacto;
- recomendación de controles: identificar las acciones costo-efectivas que podrían mitigar el riesgo. Las medidas de protección que deben formar parte del enfoque de gestión de riesgos de la empresa pueden implicar una combinación de disuasión, prevención, evasión, eliminación, detección, recuperación y corrección (**Kissel**, 2013);
- determinación del riesgo: resultado de combinar la probabilidad de ocurrencia y el impacto de la amenaza, junto con la vulnerabilidad existente;
- documentación de los resultados y elaboración de un plan de acción.

> Evaluación del riesgo (*risk assessment*) es el proceso de identificar los riesgos de seguridad de un sistema y determinar su probabilidad de ocurrencia, su impacto, y los mecanismos que mitiguen ese impacto

Figura 5. Relaciones entre los componentes del riesgo. Adaptado de **Farn**, **Lin** y **Fung** (2004).

3.3. Incidentes de seguridad

También mencionados en la bibliografía como eventos o fallas de seguridad, siguen aumentando en frecuencia y sofisticación (**Johnston**; **Warkentin**, 2010; **Nazareth**; **Choi**, 2015). La mayoría corresponden a aspectos técnicos como violaciones a los sistemas de información y redes (**Kraemer**; **Carayon**; **Clem**, 2006), en parte debido a que los consumidores presionan por un mayor acceso a los datos y aplicaciones en un mundo cada vez más conectado, lo que origina que se incrementen las oportunidades de ataques en las brechas de seguridad de estos sistemas y redes (**Nazareth**; **Choi**, 2015).

Las pérdidas debidas a fallos de seguridad de la información son notoriamente difíciles de medir (**Kannan**; **Rees**; **Sridhar**, 2007). Los autores que han tratado el tema se han centrado en mejorar la comprensión de las amenazas a la seguridad de la información a fin de que los profesionales puedan tomar mejores decisiones para hacer frente a estas amenazas (**Kraemer**; **Carayon**; **Clem**, 2006; **Li**; **Wei**, 2004; **Goodall**; **Lutters**; **Komlodi**, 2009). Las inversiones de seguridad suelen ser una respuesta a la percepción y materialización de amenazas en lugar de ser una respuesta a análisis rigurosos de la eficacia de las soluciones, controles o medidas para este tipo de amenazas (**Cremonini**; **Martini**, 2005).

En cuanto a las causas que originan los incidentes de seguridad en las organizaciones, **Beautement** *et al.* (2008) afirman que un gran número de incidentes ocurren como resultado de los fracasos de los empleados en el cumplimiento de las políticas de seguridad. La causa más común son errores no intencionados, pero existe evidencia de que en algunos casos los empleados eligen no esforzarse en cumplir con las tareas de gestión de seguridad. Al indagar sobre las razones de los no cumplimientos, la mayoría lo justifica con el impacto que estas medidas tienen en la productividad personal y organizativa, la percepción de ausencia de riesgo y el hecho de que otros compañeros de trabajo tampoco las cumplan (**Weirich**; **Sasse**, 2005; **Beautement** *et al.*, 2008).

3.4. Sistemas de información y redes

La seguridad de la información es una condición que resulta de la creación y el manteni-

miento de las medidas de protección que permiten a una empresa llevar a cabo sus funciones a pesar de los riesgos planteados por las amenazas a la disponibilidad de los sistemas de información (**Cruz-Zapata**; **Fernández-Alemán**; **Toval**, 2015). Se reconoce que las organizaciones son dependientes de los sistemas de información, las telecomunicaciones, el comercio electrónico y la tecnología, por lo que serán los delitos informáticos y otros riesgos de sistemas de información, lo que resulta en la creciente necesidad de seguridad (**Herath**; **Herath**; **Bremser**, 2010).

> El *cloud computing* (CC) o computación en la nube ha ayudado a reducir los costes de implementar más ordenadores, pero ha dado lugar a nuevos riesgos

Una de las soluciones tecnológicas más comunes, *cloud computing* (CC) o computación en la nube, ha ayudado a reducir los costes de potenciar o implementar más ordenadores, pero ha dado lugar a nuevos riesgos y a la necesidad de reevaluar y redefinir los problemas de seguridad existentes (**Albakri** *et al.*, 2014; **Zissis**; **Lekkas**, 2012). Conlleva una pérdida de control sobre la información (*Autoridad Catalana de Protección de Datos*, 2010), lo cual es contrario a lo planteado por las normas de evaluación de riesgo más populares, tales como *ISO 27005*, *NIST SP800-30*, y *AS/NZS* (*Australia Standards / New Zealand Standards*) *4360*. Estas normas suponen que los activos de una organización estén totalmente gestionados por la propia organización y que todos los procesos de gestión de la seguridad sean impuestos por la organización, pero no se aplican a los entornos informáticos en la nube (**Albakri** *et al.*, 2014). Por lo cual, dentro de la investigación sobre seguridad de la información, los sistemas de información y activos relacionados son el común denominador en los análisis de riesgos. Son éstos los principales objetivos de los ataques por parte de los criminales informáticos. Por ejemplo, la norma *ISO/IEC DIS 27017* es un estándar en curso (*ISO*, 2015) que está siendo diseñado específicamente para servicios en la nube y define directrices para apoyar la interpretación y aplicación de los controles de seguridad de la información en la nube, lo que complementa la orientación en la norma *ISO/IEC 27002* (**Cruz Zapata**; **Fernández-Alemán**; **Toval**, 2015).

3.5. Recursos humanos

El rol de las personas es vital para el éxito de cualquier organización, pero son el eslabón más débil en seguridad de la información (**Vroom**; **Von-Solms**, 2004; **Bulgurcu**; **Cavusoglu**; **Benbasat**, 2010). Según **Aurigemma** y **Panko** (2012), para combatir posibles amenazas las organizaciones se basan en políticas de seguridad de la información para orientar las acciones de los empleados. Por desgracia, las violaciones de dichas políticas por parte de los empleados son comunes y suficientes como para que a menudo se consideren no sólo el eslabón más débil en la seguridad de la información sino además el más costoso. Esto explica que gran parte de la bibliografía se haya dedicado al comportamiento de los usuarios de la información. **Thomson**, **Von-Solms** y **Louw** (2006) enfatizan que los empleados sepan y estén entrenados en las habilidades necesarias para proteger los activos de información, como parte de su práctica diaria. Después de décadas de acercamientos meramente técnicos, ahora es aceptado ampliamente que "las personas son la piedra angular de la seguridad de la información" (**Bishop**; **Frincke**, 2005), y juegan un papel central en las medidas de seguridad y la toma de decisiones. Según **Proctor** y **Chen**, (2015) es crucial la investigación sobre las decisiones humanas relacionadas con la seguridad y las acciones basadas en los principios de procesamiento humano de la información. Varios autores confirman la importancia de convertir las políticas de seguridad de la información en comportamientos cotidianos de los empleados, es decir, trabajar en la construcción de una cultura organizativa de seguridad de la información (**Von-Solms**; **Von-Solms**, 2004b; **Von-Solms**, 2000). Además, ven la necesidad de cambiar el enfoque en tecnología por un enfoque en las personas (**Kayworth**; **Whitten**, 2010; **Johnson**; **Goetz**, 2007). De los enfoques para el cumplimiento de las políticas de seguridad de la información, la formación es el más comúnmente sugerido en la bibliografía (**Puhakainen**; **Siponen**, 2010; **Von-Solms**; **Von-Solms**, 2004b).

> Es importante trabajar en la construcción de una cultura organizativa de seguridad de la información

Otro aspecto destacable en la bibliografía es la relación entre la cultura de seguridad de la información y la cultura corporativa, resaltando que ambas deben estar alineadas y que se influencian mutuamente (**Chang**; **Lin**, 2007; **Lim** *et al.*, 2009). En temas de ciberseguridad, la actitud displicente de las personas hacia la seguridad hace que sean el eslabón más débil de la cadena (**Furnell**; **Thomson**, 2009). Se plantea a menudo son ignorantes e ingenuos acerca de los problemas de seguridad de información a los que están expuestos (**Furnell**; **Thomson**, 2009). En la bibliografía se plantea como buena práctica realizar programas de sensibilización, evitando usar el mismo mensaje de concienciación para categorías de usuarios de internet (**Valentine**; **Labs**, 2006). Se recomienda diseñar un programa de sensibilización eficaz que se adapte a los distintos destinatarios debido a la variación en el conocimiento de seguridad, comportamiento, mentalidad hacia la protección online, tecnología empleada, fuente de acceso a internet y nivel de aceptación (**Choo**, 2011; **Johnson**, 2006).

3.6. Aspectos económicos

La seguridad de la información, que antes se consideraba solamente como gastos generales, es reconocida ahora como una inversión estratégica para las empresas. Las iniciativas de seguridad requieren de una buena gestión y a su vez de esfuerzos económicos, puesto que el costo de la implementación de mejores prácticas como solución a los problemas es de enormes proporciones para la mayoría de las organizaciones. A medida que éstas van comprometiendo mayor cantidad de recursos, el equipo responsable se enfrenta a menudo a justificar estas inversiones y responder a muchas preguntas sobre su valor, por ejemplo:

- ¿vale la pena la inversión?
- ¿hay que utilizar proveedores externos de seguridad o implementar soluciones de seguridad interna?
- ¿los mecanismos de seguridad han sido implementados con éxito?
- ¿cómo podemos estar preparados para los futuros cambios y desafíos? (**Herath**; **Herath**; **Bremser**, 2010).

Con este telón de fondo, y después de analizar la compensación de la inversión económica (tales como servidores de seguridad mejorados y sistemas de detección de intrusos), **Gordon** y **Loeb** (2006) sugieren tener en cuenta las siguientes preguntas para decidir asignar presupuesto a la seguridad de la información

- ¿cuánto debe una organización gastar en seguridad de la información?
- ¿cómo debería una organización asignar su presupuesto de seguridad de la información a las actividades específicas de seguridad?
- ¿cuál es el costo económico de las brechas de seguridad de información?

Bojanc y **Jerman-Blažič** (2008) analizan varios enfoques para evaluar las inversiones necesarias en tecnología de seguridad desde el punto de vista económico. Presentan además métodos para identificación de activos, amenazas y vulnerabilidades de los sistemas de TIC, y proponen un procedimiento de selección de la inversión óptima de tecnología de seguridad basado en la cuantificación de los valores de los sistemas protegidos. De la misma manera, **Salmela** (2007) examina el uso de análisis de procesos de negocio como un método para asociar los riesgos de los sistemas de información con las pérdidas potenciales.

3.7. Gobernanza de seguridad de la información

"El gobierno corporativo se refiere al proceso a través del cual se toman las decisiones y el proceso por el que las decisiones son implementadas" (*Comisión Económica y Social*, s.f.).

Al hablar de gobernanza corporativa se hace referencia al compromiso de la dirección ejecutiva de una compañía y consiste en "un conjunto de políticas y controles internos por los cuales se dirigen y gestionan las organizaciones, sin importar su tamaño" (*National Cyber Security*, 2004).

Del mismo modo, la gobernanza de seguridad de la información describe el proceso por el cual se aborda la seguridad de la información desde un nivel ejecutivo en la organización. Varios autores (**Posthumus**; **Von-Solms**, 2004; **Von-Solms**; **Von-Solms**, 2005), muestran que la seguridad de la información debe ser una prioridad de la dirección ejecutiva; por lo tanto debe comenzar como una responsabilidad de gobierno corporativo. Esto establece la necesidad de integrar la seguridad de la información en la dirección corporativa a través del desarrollo de un marco de gobierno de la seguridad de la información.

De acuerdo con **Von-Solms** (2006), la gobernanza de seguridad de la información es parte de la gobernanza corporativa. Por otra parte, **Knapp** *et al.* (2009) la presentan como un componente general que afecta directamente a todas las etapas del proceso de gestión de política de seguridad de la información, insistiendo en que no es solamente un proceso interno de la organización, sino que también puede incluir la participación de entes externos tales como el comité directivo.

3.8. Políticas

Existe acuerdo en que una buena política de seguridad de información es la base para la misma en las organizaciones (**Baskerville**; **Siponen**, 2002; **Knapp** *et al.*, 2009; **Von-Solms**; **Von-Solms**, 2004a; **David**, 2002). Según **David** (2002), "sin políticas de seguridad formales, la seguridad es arbitraria, sujeta a los caprichos de aquellos que la administran".

Los resultados de la evaluación y análisis de riesgos deben conducir a la elaboración de la política de seguridad, que consiste en un documento que indica el compromiso y apoyo de la dirección, así como la definición del papel que debe jugar en la consecución de la misión y visión de la organización. En esencia se documenta para explicar la necesidad de seguridad de la información (y sus principios) a todos los usuarios de los recursos de información (**Höne**; **Eloff**, 2002).

Entre los aspectos que debería contener ese documento se encuentran (**Doherty**; **Fulford**, 2006; **Höne**; **Eloff**, 2002; **Lindup**, 1995):

- definición de seguridad para los activos de información;
- responsabilidades;
- planes de contingencia;
- gestión de contraseñas;
- sistema de control de acceso;
- control de acceso;
- manejo de virus e intrusos.

Además, se debe incluir el reporte de incidentes de seguridad, sobre el cual se deben establecer lineamientos claros dentro de la política de seguridad de la compañía (**Wiant**, 2005).

Para la elaboración de las políticas se debe contar con la participación activa de los colaboradores o miembros de la organización, involucrando las actividades de éstos y el entorno de trabajo. Según **Karyda**, **Kiountouzis** y **Kokolakis** (2005), los tres procesos involucrados en la adopción de una política de seguridad son: formulación, implementación y adopción (figura 6).

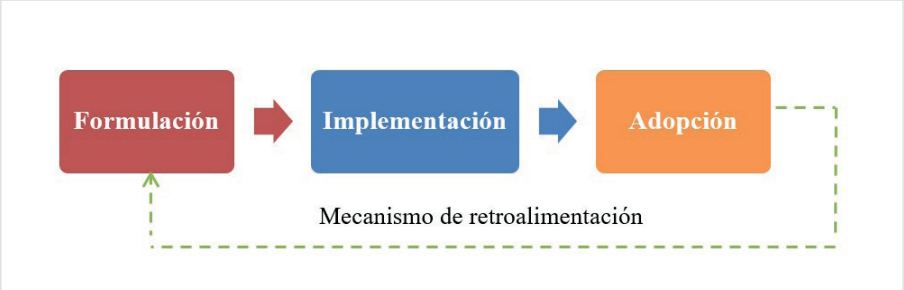

Figura 6. Proceso de aplicación de una política de seguridad, a partir de **Karyda**, **Kiountouzis** y **Kokolakis** (2005).

Las políticas de seguridad de la información ayudan a los usuarios a garantizar la seguridad cuando se usan tecnologías de la información y demás recursos (**Aurigemma**; **Panko**, 2012; **Whitman**; **Townsend**; **Aalberts**, 2001, citado por **Aurigemma**; **Panko**, 2012). Además, describen las funciones y responsabilidades de los empleados, y abordan las cuestiones específicas de seguridad, en la protección de los recursos de información de su organización (**Bulgurcu**; **Cavusoglu**; **Benbasat**, 2010).

3.9. Buenas prácticas

Las buenas prácticas (*best practices*) "definen prácticas y procedimientos que permitan crear un ambiente consistente que sea seguro mientras siga siendo útil" (*Information Security Best Practices*, s.f.).

En casi todas las áreas del conocimiento y del mundo económico se requieren estándares que permitan establecer bases y criterios para la excelencia. El campo de la seguridad de la información no es la excepción.

Según **Von-Solms** (2000), las buenas prácticas internacionales para la gestión de la seguridad de la información (GSI) son la compilación de experiencias combinadas de muchas compañías internacionales influyentes, acerca de la forma en que gestionan la seguridad de la información. Estas prácticas reflejan la experiencia de dichas compañías sobre las medidas de control relevantes, procedimientos y técnicas, que proporcionan un nivel adecuado o aceptable de seguridad de la información.

Además, las buenas prácticas proveen un marco de trabajo como referencia para asegurar que las organizaciones cubran todas las bases de seguridad de la información. Uno de los documentos más conocidos de este tipo es la serie *ISO/IEC 27000*, también conocida como la familia de estándares del sistema de gestión de seguridad de la información (SGSI), que ofrece recomendaciones y plantea riesgos y controles aplicables a todas las organizaciones, independientemente del tipo, tamaño y naturaleza.

También está alineada con la norma *ISO 9001* e *ISO 14001* con el fin de apoyar la aplicación coherente e integrada y permitir a una organización alinear su SGSI con los requisitos relacionados del sistema de gestión (**Mesquida**; **Mas**, 2015).

La familia *ISO/IEC 27000* incluye la *ISO/IEC 27001*, que tiene un enfoque organizacional y detalla los requerimientos con los cuales se puede auditar el SGSI, además de ser el único esquema de aceptación internacional que permite certificación. Por otro lado incluye también la *ISO/IEC 27002* que está más centrada en el individuo y proporciona un código de buenas prácticas para uso de las personas dentro de una organización, al tiempo que puede servir para ayudar a construir la confianza en las actividades inter-organizacionales (*ISO*, 2005). La *ISO/IEC 27002* es el cambio de nombre de la norma *ISO/IEC 17799* y, contiene 14 cláusulas de control de seguridad que contienen colectivamente un total de 35 categorías de seguridad y 114 controles de alto nivel que abarcan tanto las amenazas externas como internas (**Mesquida**; **Mas**, 2015). Podría requerirse considerar otros controles de seguridad, no incluidos en *ISO/IEC 27002*, para proveer mayor protección, especialmente para activos de gran valor o para contrarrestar niveles excepcionalmente altos de las amenazas de seguridad (**Von-Solms**, 2001).

Finalmente es importante mencionar el concepto de conformidad, que es el proceso práctico de comparar los controles aplicados en una organización con aquellos propuestos en *ISO/IEC 27002*. Es básicamente un análisis de brechas en el cual se descubren las diferencias entre la situación de la organización y el estándar. Al respecto, **Karabacak** y **Sogukpinar** (2006) proponen un método cuantitativo basado en una encuesta que evalúa la conformidad de *ISO/IEC 27002*. Éste tiene cualidades únicas como su facilidad de uso y flexibilidad. Se pueden cambiar fácilmente el número de preguntas, opciones de respuesta y ajustar los valores numéricos para las mismas.

4. Conclusiones

Estudios previos, como **Hong** *et al.* (2003), sugieren que la ausencia de un marco y una metodología han contribuido a la falta de teoría en GSI. De la misma manera, *Entrust* (2004) sugiere que existen muy pocos marcos de trabajo sobre seguridad de información que puedan guiar efectivamente a la mayoría de las organizaciones en sus esfuerzos de GSI (gestión de seguridad de la información). Se han analizado elementos relacionados con la base teórica necesaria para un marco de trabajo integral de la GSI en las organizaciones.

La aportación significativa de este documento es la clasificación de las variables estratégicas del sistema de investigación en el área de seguridad de la información y el desarrollo de un lenguaje común para ello, con el fin de dilucidar los componentes que debe tener en cuenta el nivel ejecutivo para el éxito de los esfuerzos de seguridad de la información de una organización. Por supuesto, este marco debe integrarse con otros puntos de vista a fin de lograr una comprensión holística del tema.

Se sugiere como opción utilizar un marco de seguridad particular que considere tanto las características propias de la organización como los factores o categorías sugeridas en este marco y otros ya existentes. Para ello se debe tener en cuenta el tipo de requerimientos de la industria o de cumplimiento, ya que podrían ser factores decisivos.

Por otra parte, la serie *ISO 27000* es la obra magna de marcos de seguridad de la información con aplicabilidad en cualquier industria, aunque el proceso de implementación es largo y complicado. Sin embargo, se utiliza mejor cuando la empresa necesita dar brillo a su imagen y comercializar sus capacidades de seguridad de la información a través de la certificación *ISO 27000*. De manera similar, el *NIST SP 800-53* es el estándar requerido por las agencias federales de Estados Unidos, pero también podría ser utilizado por cualquier empresa para construir un plan de seguridad de la información relativo a tecnologías. Cualquiera de ellos apoya la función de un profesional de la seguridad para organizar y gestionar un programa de seguridad de la información (**Granneman**, 2013).

Por otra parte, se contribuye teóricamente a la bibliografía de la GSI, principalmente por el análisis y estructuración de las palabras clave identificadas en los artículos obtenidos de

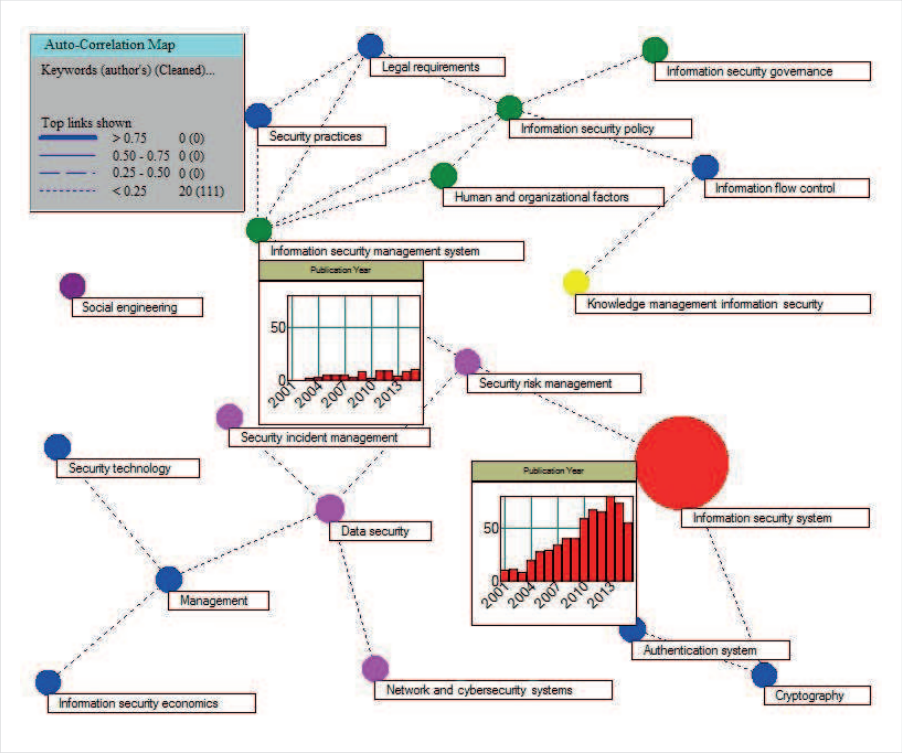

Figura 7. Mapa de autocorrelación de las *keywords* o descriptores de la búsqueda "*Information security*". Se ha usado *Vantange point*. Octubre de 2015.

la búsqueda, de acuerdo con la frecuencia y asociatividad de las mismas. Esto es, se proponen 9 categorías sobre las cuales se han encontrado evidencias de su relación entre ellas, y su relación con el grupo de controles de primer nivel que proponen los estándares internacionales sobre el sistema de GSI. Dicha evidencia se ilustra en el mapa de autocorrelación, que muestra las palabras claves con mayor número de frecuencia medido por el número de registros que mencionan estas *keywords* y refleja la similitud o relación entre estos descriptores mediante las líneas entre ellos (lo que significa que los autores han escrito en un mismo artículo usando las *keywords* asociadas). La figura 7 representa este conjunto de datos analizados, donde cada nodo representa un descriptor, y el tamaño del nodo refleja el número de registros asociados con el descriptor. Todos los nodos son iguales porque los descriptores tienen un número similar de registros, excepto "*Information security system".*

> Es necesario integrar la seguridad de la información en la gestión empresarial a través del desarrollo de un marco de gobernanza

Se puede argumentar que las organizaciones deben utilizar el marco presentado en este documento con el fin de poner algo de estructura en un área intrínsecamente no estructurada como es la GSI. Teniendo en cuenta que la información se ha convertido en una fuente de riqueza y de riesgo para las compañías (la protejan activamente o no), los miembros involucrados en la gestión de información necesitan entender la complejidad e importancia de su aseguramiento.

Por lo tanto es necesario integrar la seguridad de la información en la gestión empresarial a través del desarrollo de un marco de gobernanza. En especial, cuando se nota que a pesar del esfuerzo por cambiar el enfoque técnico por un enfoque de gestión, aún las evaluaciones de riesgo están encaminadas a la identificación de amenazas técnicas. Lo anterior se refleja en el comportamiento de las publicaciones. Según un informe de **Li** (2015) que evalúa la información divulgada sobre seguridad de la información basada en las 26 palabras claves de seguridad sugeridas por **Gordon**, **Loeb** y **Sohail** (2010), describiendo el número de veces que se encontraba cada una de estas palabras claves al examinar los párrafos en los reportes anuales analizados, las prácticas "*Business continuity*" y "*Security management*" son las más comunes en las empresas ocupando el segundo y tercer lugar en la lista. **Herath** (2008) advierte que la investigación empírica sobre las conductas en los usuarios de la información y los factores que influyen en ellas apenas ha comenzado. El motivo de la ausencia de una base teórica y un acercamiento formal a la GSI no se conoce. Según **Mercer** (2004, citado por **Li**, 2015) puede ser debido a la falta de credibilidad en los estudios realizados sobre seguridad de la información.

Se concluye finalmente que futuras investigaciones podrían estar encaminadas hacia los riesgos correspondientes al capital intelectual más allá de la misma información.

Notas

1. El análisis de contenido "es una técnica de investigación para la descripción objetiva, sistemática y cuantitativa del contenido manifiesto de las comunicaciones, teniendo como fin interpretarlos" (**Pinto**; **Grawitz**, 1967).

2. El *National Institute of Standards and Technology* (*NIST*) fue fundado en 1901 y ahora forma parte del *Department of Commerce* de los Estados Unidos. *NIST* es uno de los laboratorios de ciencias físicas más antiguos de la nación. *https://www.nist.gov*

5. Bibliografía

Aimeur, Esma; **Schonfeld, David** (2011). "The ultimate invasion of privacy: identity theft". In: *9th Annual intl conf on privacy, security and trust*, pp. 24-31.
http://www.site.uottawa.ca/~nelkadri/CSI5389/Papers/8-Aimeur_and_Schonfeld_PST2011.pdf

Albakri, Sameer-Hasan; **Shanmugam, Bharanidharan**; **Samy, Ganthan-Narayana**; **Idris, Norbik-Bashah**; **Ahmed, Azuan** (2014). "Security risk assessment framework for cloud computing environments". *Security and communication networks*, v. 7, n. 11, pp. 2114-2124.
https://doi.org/10.1002/sec.923

Albrechtsen, Eirik (2007). "A qualitative study of users' view on information security". *Computers & security*, v. 26, n. 4, pp. 276-289.
https://goo.gl/yzJWcu
https://doi.org/10.1016/j.cose.2006.11.004

Atkinson, Shirley; **Furnell, Steven**; **Phippen, Andy** (2009). "Securing the next generation: enhancing e-safety awareness among young people". *Computer fraud & security*, v. 2009, n. 7, pp. 13-19.
https://goo.gl/PncpO6
https://doi.org/10.1016/S1361-3723(09)70088-0

Aurigemma, Salvatore; **Panko, Raymond** (2012). "A composite framework for behavioral compliance with information security policies". In: *45th Hawaii intl conf on system sciences*, pp. 3248-3257. IEEE.
https://goo.gl/I433tj
https://doi.org/10.1109/HICSS.2012.49

Autoridad Catalana de Protección de Datos (2010). "Conclusiones de 'La coordinación de la protección de datos en el sector público y privado. La figura del *data protection officer*'". *Apdcat. Autoridad Catalana de Protección de Datos*, 18 octubre.
http://apdcat.org/es/noticia.php?cat_id=226&not_id=301

Baskerville, Richard; **Siponen, Mikko** (2002). "An information security meta-policy for emergent organizations". *Logistics information management*, v. 15, n. 5/6, pp. 337-346.
https://www.researchgate.net/publication/250915970_An_information_security_meta-policy_for_emergent_organizations
https://doi.org/10.1108/09576050210447019

Beautement, Adam; **Coles, Robert**; **Griffin, Jonathan**; **Ioannidis, Christos**; **Monahan, Brian**; **Pym, David**; **Sasse, Angela**; **Wonham, Mike** (2008). "Modelling human and technological costs and benefits of USB memory stick security". In: *Workshop on economics in information security*, pp. 1-57.
http://www.econinfosec.org/archive/weis2008/papers/Pym.pdf
http://dblp2.uni-trier.de/db/conf/weis/

Bishop, Matt; **Frincke, Deborah** (2005). "A human endeavor: Lessons from Shakespeare and beyond". *IEEE security & privacy magazine*, v. 3, n. 4, pp. 49-51.
https://doi.org/10.1109/MSP.2005.87

Bojanc, Rok; **Jerman-Blažič, Borka** (2008). "An economic modeling approach to information security risk management". *International journal of information management*, v. 28, n. 5, pp. 413-422.
https://goo.gl/1ko0DG
https://doi.org/10.1016/j.ijinfomgt.2008.02.002

Broadhurst, Roderic; **Chang, Lennon Y. C.** (2013). "Cybercrime in Asia: Trends and challenges". In: Liu, Jianhong; Hebenton, Bill; Jou, Susyan (eds.). *Handbook of Asian criminology, Part I*. Springer: New York, pp. 49-63. ISBN: 978 1461452171
https://doi.org/10.1007/978-1-4614-5218-8_4

Brynjolfsson, Erik; **Hitt, Lorin** (1996). "Paradox lost? Firm-level evidence on the returns to information systems spending". *Management science*, v. 42, n. 4.

Citado por **Doherty, Neil**; **Anastasakis, Leonidas**; **Fulford, Heather** (2009). "The information security policy unpacked: a critical study of the content of university policies". *International journal of information management*, v. 29, n. 6, pp. 449-457.
https://doi.org/10.1016/j.ijinfomgt.2009.05.003

Bulgurcu, Burcu; **Cavusoglu, Hasan**; **Benbasat, Izak Benbasat** (2010). "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness". *MIS quarterly*, v. 34, n. 3, pp. 523-548.
http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2919&context=misq

CERT (s.f.). *Octave.* Software Engineering Institute – Carnegie Mellon University.
http://www.cert.org/octave

Chang, Shuchih E.; **Lin, Chin-Shien** (2007). "Exploring organizational culture for information security management". *Industrial management & data systems*, v. 107, n. 3, pp. 438-458.
https://goo.gl/DooZl7
https://doi.org/10.1108/02635570710734316

Choo, Kim-Kwang-Raymond (2011). "The cyber threat landscape: challenges and future research directions". *Computers & security*, v. 30, n. 8, pp. 719-731.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2339821
https://doi.org/10.1016/j.cose.2011.08.004

Cole, Jeffrey I.; **Suman, Michael**; **Schramm, Phoebe**; **Zhou, Liuning**; **Salvador, Andromeda** (2013). *The digital future project 2013. Surveying the digital future. Year eleven.* Los Angeles, CA: Center for the Digital Future.
http://www.digitalcenter.org/wp-content/uploads/2013/06/2013-Report.pdf

Cremonini, Marco; **Martini, Patrizia** (2005). "Evaluating information security investments from attackers perspective: The return-on-attack (ROA)". In: *4th Workshop on the economics of information security*, p. 4.
https://goo.gl/VRTVee

Cruz-Zapata, Belén; **Fernández-Alemán, José-Luis**; **Toval, Ambrosio** (2015). "Security in cloud computing: A mapping study". *Computer science and information systems*, v. 12, n. 1, pp. 161-184.
https://doi.org/10.2298/CSIS140205086C

Da-Veiga, Adéle; **Martins, Nico** (2015). "Information security culture and information protection culture: A validated assessment instrument". *Computer law & security review*, v. 31, n. 2, pp. 243-256.
https://doi.org/10.1016/j.clsr.2015.01.005

David, Jon (2002). "Policy enforcement in the workplace". *Computers & security*, v. 21, n. 6, pp. 506-513.
https://doi.org/10.1016/S0167-4048(02)01006-4

Desouza, Kevin C.; **Vanapalli, Ganesh K.** (2005). "Securing knowledge in organizations: Lessons from the defense and intelligence sectors". *International journal of information management*, v. 25, n. 1, pp. 85-98.
https://doi.org/10.1016/j.ijinfomgt.2004.10.007

Dhillon, Gurpreet (2001). "Violation of safeguards by trusted personnel and understanding related information security concerns". *Computers & security*, v. 20, n. 2, pp. 165-172.
https://doi.org/10.1016/S0167-4048(01)00209-7

Dlamini, Moses T.; **Eloff, Jan H. P.**; **Eloff, Mariki M.** (2009). "Information security: the moving target". *Computers & security*, v. 28, n. 3-4, pp. 189-198.
https://doi.org/10.1016/j.cose.2008.11.007

Doherty, Neil F.; **Fulford, Heather** (2006). "Aligning the information security policy with the strategic information systems". *Computers & security*, v. 25, n.1, pp. 55-63.
https://doi.org/10.1016/j.cose.2005.09.009

Doherty, Neil F.; **King, Malcolm**; **Al-Mushayt, Omar** (2003). "The impact of inadequacies in the treatment of organizational issues on information systems development projects". *Information & management*, v. 41, n. 1, pp. 49-62.
https://goo.gl/SdSyYe
https://doi.org/10.1016/S0378-7206(03)00026-0

Dolan, Paul; **Shaw, Rebecca**; **Tsuchiya, Aki**; **Williams, Alan** (2005). "QALY maximisation and people's preferences: A methodological review of the literature". *Health economics*, v. 14, n. 2, pp. 197-208.
http://eprints.gla.ac.uk/4190/1/4190.pdf
https://doi.org/10.1002/hec.924

Drucker, Peter F. (1988). "The coming of the new organization". *Harvard business review*, v. 66, n. 1, pp. 47.
https://hbr.org/1988/01/the-coming-of-the-new-organization

Entrust, Inc. (2004). *Information security governance (ISG). An essential element of corporate governance*. Entrust securing digital identities & information.
https://www.entrust.com/wp-content/uploads/2013/05/wp_entrust_isg_april04.pdf

Farn, Kwo-Jean; **Lin, Shu-Kuo**; **Fung, Andrew-Ren-Wei** (2004). **"**A study on information security management system evaluation -assets, threat and vulnerability". *Computer standards& interfaces*, v. 26, n. 6, pp. 501-513.
https://goo.gl/qU5lcj
https://doi.org/10.1016/j.csi.2004.03.012

Furnell, Steven (2008). "End-user security culture: A lesson that will never be learnt?". *Computer fraud & security*, n. 4, pp. 6-9.
https://goo.gl/7i9Rrp
https://doi.org/10.1016/S1361-3723(08)70064-2

Furnell, Steven; **Thomson, Kerry-Lynn** (2009). "From culture to disobedience: Recognising the varying user acceptance of IT security". *Computer fraud & security*, n. 2, pp. 5-10.
https://goo.gl/FQdi7e
https://doi.org/10.1016/S1361-3723(09)70019-3

Gerber, Mariana; **Von-Solms, Rossouw** (2005)**.** "Management of risk in the information age". *Computers & security*, v. 24, n. 1, pp. 16-30.
https://www.researchgate.net/publication/222827356_Management_of_risk_in_the_information_age
https://doi.org/10.1016/j.cose.2004.11.002

Goodall, John R.; **Lutters, Wayne G.**; **Komlodi, Anita** (2009). "Developing expertise for network intrusion detection". *Information technology & people*, v. 22, n. 2, pp. 92-108.
http://dx.doi.org/10.1108/09593840910962186

Gordon, Lawrence A.; **Loeb, Martin P.** (2006). "Economic aspects of information security: An emerging field of research". *Information systems frontiers*, v. 8, n. 5, pp. 335-337.
https://pdfs.semanticscholar.org/5cbe/0a86b1b1c8e5f2327592f44351943f57d82b.pdf
https://doi.org/10.1007/s10796-006-9010-7

Gordon, Lawrence A.; **Loeb, Martin P.**; **Sohail, Tashfeen** (2010). "Market value of voluntary disclosures concerning information security". *MIS quarterly*, v. 34, n. 3, pp. 567-594.
http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2921&context=misq

Granneman, Joseph (2013). "IT security frameworks and standards: Choosing the right one". *TechTarget search security*, Sept.
http://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

Gross, Joshua B.*;* **Rosson, Mary-Beth** (2007). "Looking for trouble: understanding end-user security management". In: *Chimit. Procs of the 2007 Symposium on computer human interaction for management of information technology*, art. n. 10.
https://www.researchgate.net/publication/221545618_Looking_for_trouble_Understanding_end-user_security_management
http://dx.doi.org/10.1145/1234772.1234786

Gutiérrez, Javier J. (s.f.). ¿Qué es un framework web?
http://www.lsi.us.es/~javierj/investigacion_ficheros/Framework.pdf

Halliday, Sharon; **Badenhorst, Karin**; **Von-Solms, Rossouw** (1996). "A business approach to effective information technology risk analysis and management". *Information management & computer security*, v. 4, n. 1, pp.19-31.
http://dx.doi.org/10.1108/09685229610114178

Herath, Tejaswini (2008). *Essays on information security practices in organizations*. State University of New York at Buffalo: ProQuest Dissertations Publishing.
http://search.proquest.com/docview/304383191

Herath, Tejaswini; **Herath, Hemantha**; **Bremser, Wayne G.** (2010). "Balanced scorecard implementation of security strategies: A framework for IT security performance management". *Information systems management*, v. 27, n. 1, pp. 72-81.
https://doi.org/10.1080/10580530903455247

Höne, Karin; **Eloff, Jan H. P.** (2002). "Information security policy – what do international information security standards say?". *Computers & security*, v. 21, n. 5, pp. 402-409.
https://doi.org/10.1016/S0167-4048(02)00504-7

Hong, Kwo-Shing; **Chi, Yen-Ping**; **Chao, Louis R.**; **Tang, Jih-Hsing** (2003). "An integrated system theory of information security management". *Information management & computer security*, v. 11, n. 5, pp. 243-248.
https://goo.gl/5pvYbj
https://doi.org/10.1108/09685220310500153

ISO (2005). *ISO/IEC 27002:2005. Information technology. Security techniques. Code of practice for information security management*. International Standards Organization, 15 June.
http://www.iso.org/iso/catalogue_detail?csnumber=50297

ISO (2015). *ISO/IEC DIS 27017. Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. International Standards Organization, 15 Dec.
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757

Johnson, Everett C. (2006). "Security awareness: switch to a better programme". *Network security*, n. 2, pp. 15-18.
https://goo.gl/KVQMGF
https://doi.org/10.1016/S1353-4858(06)70337-3

Johnson, M. Eric; **Goetz, Eric** (2007). "Embedding information security into the organization". *IEEE security & privacy magazine*, v. 5, n. 3, pp. 16-24.
http://www.ists.dartmouth.edu/library/352.pdf
https://doi.org/10.1109/MSP.2007.59

Johnston, Allen C.; **Warkentin, Merrill** (2010). "Fear appeals and information security behaviors: an empirical study". *MIS quarterly*, v. 34, n. 3, pp. 549-566.
http://dl.acm.org/citation.cfm?id=2017478

Kannan, Karthik; **Rees, Jackie**; **Sridhar**; **Sanjay** (2007). "Market reactions to information security breach announcements: An empirical analysis". *International journal of electronic commerce*, v. 12, n. 1, pp.69-91.
https://goo.gl/u1DMg9
https://doi.org/10.2753/JEC1086-4415120103

Knapp, Kenneth J.; **Morris Jr, R. Franklin**; **Marshall, Thomas E.**; **Byrd, Terry-Anthony** (2009). "Information security policy: An organizational-level process model". *Computers & security*, v. 28, n. 7, pp. 493-508.
https://goo.gl/qB7S5p
https://doi.org/10.1016/j.cose.2009.07.001

Karabacak, Bilge; **Sogukpinar, Ibrahim** (2006). "A quantitative method for *ISO 17799* gap analysis". *Computers & security*, v. 25, n. 6, pp. 413-419.
https://goo.gl/sPbVcZ
https://doi.org/10.1016/j.cose.2006.05.001

Karyda, Maria; **Kiountouzis, Evangelos**; **Kokolakis, Spyros** (2005). "Information systems security policies: a contextual perspective". *Computers & security*, v. 24, n. 3, pp. 246-260.
https://goo.gl/oaSvNb
https://doi.org/10.1016/j.cose.2004.08.011

Kayworth, Tim; **Whitten, Dwayne** (2012). "Effective information security requires a balance of social and technology factors". *MIS quarterly executive*, v. 9, n. 3, pp. 163-175.
https://ssrn.com/abstract=2058035

Kissel, Richard (2013). *Glossary of key information security terms*. *Nistir 7298, Revision 2.* Gaithersburg: National Institute of Standards and Technology, Computer Security Division, & Information Technology Laboratory, Eds.
https://doi.org/10.6028/NIST.IR.7298r2

Kraemer, Sara; **Carayon, Pascale**; **Clem, John F.** (2006). "Characterizing violations in computer and information security systems". In: *Procs of the 16th Triennial world congress of the International Ergonomics Association (IEA).*
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.570.5398&rep=rep1&type=pdf

Kruger, Hennie A.; **Kearney, Wayne D.** (2006). "A prototype for assessing information security awareness". *Computers & security*, v. 25, n. 4, pp. 289-296.
https://doi.org/10.1016/j.cose.2006.02.008

Lategan, Neil; **Von-Solms, Rossouw** (2006). "Towards enterprise information risk management: a body analogy". *Computer fraud & security*, n. 12, pp. 15-19.
https://goo.gl/Cl0qSY
https://doi.org/10.1016/S1361-3723(06)70453-5

Layton, Timothy P. (2007). *Information security: Design, implementation, measurement and compliance*. New York: Auerbach Publications, Taylor & Francis Group. ISBN: 978 0849370878

Leiner, Barry M.; **Cerf, Vinton G.**; **Clark, David D.**; **Kahn, Robert E.**; **Kleinrock, Leonard**; **Lynch, Daniel C.**; **Postel, Jon**; **Roberts, Lawrence G.**; **Wolff, Stephen S.** (1997). "The past and future history of the internet". *Communication of the ACM*, v. 40, n. 2, pp. 102-108.
https://goo.gl/8ciny
https://doi.org/10.1145/253671.253741

Li, David C. (2015). "Online security performances and information security disclosures". *Journal of computer information systems*, v. 55, n. 2, pp. 20-28.
https://doi.org/10.1080/08874417.2015.11645753

Li, Yi; **Wei, June** (2004). "Computer information systems threat analysis on security". In: *2004 IRMA intl conf*, pp. 951-953.
http://www.irma-international.org/viewtitle/32521/

Lim, Kwanghui (2004). "The relationship between research and innovation in the semiconductor and pharmaceutical industries (1981-1997)". *Research policy*, v. 33, n. 2, pp. 287-321.
http://kwanghui-public.s3.amazonaws.com/limrespol2004.pdf
https://doi.org/10.1016/j.respol.2003.08.001

Lim, Joo; **Chang, Shanton**; **Maynard, Sean**; **Ahmad, Atif** (2009). "Exploring the relationship between organizational culture and information security culture". In: *Procs of the 7th Australian information security management conf*, pp. 88-97.
https://doi.org/10.4225/75/57b4065130def

Lindup, Kenneth R. (1995). "A new model for information security policies". *Computers & security*, v. 14, n. 8, pp. 691-695.
https://doi.org/10.1016/0167-4048(96)81709-3

Loibl, Timothy R. (2005). "Identity theft, spyware and the law". In: *InfoSecCD '05. Procs of the 2nd annual conf on information security curriculum development*, Kennesaw, pp. 118-121.
https://doi.org/10.1145/1107622.1107650

Lu, Weisheng; **Chau, K. W.**; **Wang, Hongdi**; **Pan, Wei** (2014). "A decade's debate on the nexus between corporate social and corporate financial performance: a critical review of empirical studies 2002-2011". *Journal of cleaner production*, v. 79, pp. 195-206.
https://goo.gl/C8c1BS
https://doi.org/10.1016/j.jclepro.2014.04.072

Mell, Peter; **Grance, Timothy** (2011). *The NIST definition of cloud computing*. National Institute of Standards and Technology. Special Publication 800-145, Sept.
http://dx.doi.org/10.6028/NIST.SP.800-145

Markus, M. Lynne (2004). "Technochange management: using IT to drive organizational change". *Journal of information technology*, v. 19, n. 1, pp. 4-20.
https://doi.org/10.1057/palgrave.jit.2000002

Martínez-Acevedo, Álvaro-Javier; **Forero-Toloza, Diana-Magally**; **Pinto-Prieto, Laura-Patricia**; **Becerra-Ardila, Luis-Eduardo** (2013). "Análisis bibliométrico de la producción científica acerca de técnicas de adquisición y representación de conocimiento a través del Social Sciences Citation Index (2001-2013)". En: *Retos y desafíos de las ciudades del futuro: innovadoras, inclusivas, sostenibles y sustentables*. Bogotá: Universidad Nacional Abierta y a Distancia, pp. 259–282. ISBN: 978 9586515658
http://online.fliphtml5.com/qszg/qiqr/#p=1

Mercer, Molly (2004). "How do investors assess the credibility of management disclosures?" *Accounting horizons*, v. 18, n. 3, pp. 185-196.
https://doi.org/10.2308/acch.2004.18.3.185

Citado por: **Li, David C.** (2015). "Online security performances and information security disclosures". *Journal of computer information systems*, v. 55, n. 2, pp. 20-28.
http://dx.doi.org/10.1080/08874417.2015.11645753

Mesquida, Antoni-Lluís; **Mas, Antonia** (2015). "Implementing information security best practices on software lifecycle processes: The *ISO/IEC 15504* security extension". *Computers and security*, v. 48, pp. 19-34.
https://goo.gl/BZt89n
https://doi.org/10.1016/j.cose.2014.09.003

Mitnick, Kevin D.; **Simon, William L.**; **Wozniak, Steve** (2003). *The art of deception: Controlling the human element of security*. Indianapolis: Wiley Publishing. ISBN: 978 0764542800
http://sbisc.ut.ac.ir/wp-content/uploads/2015/10/mitnick.pdf

Modi, **Chirag**; **Patel**, **Dhiren**; **Borisaniya**, **Bhavesh**; **Patel**, **Hiren**; **Patel**, **Avi**; **Rajarajan**, **Muttukrishnan** (2013). "A survey of intrusion detection techniques in cloud". *Journal of network and computer applications*, v. 36, n. 1, pp. 42-57.
http://openaccess.city.ac.uk/1737/
https://doi.org/10.1016/j.jnca.2012.05.003

National Cyber Security Summit Task Force (2004). *Information security governance: A call to action.*
https://goo.gl/r95XIk

Nazareth, Derek L.; **Choi, Jae** (2015). "A system dynamics model for information security management". *Information & management*, v. 52, n. 1, pp. 123-134.
https://goo.gl/Ujw1g9
https://doi.org/10.1016/j.im.2014.10.009

Nnolim, Anene (2007). *A framework and methodology for information security management*. Michigan, United States: Lawrence Technological University, ProQuest Dissertations & Theses (PQDT) database; 353 pp.
http://gradworks.umi.com/32/96/3296872.html

Okuda-Benavides, Mayumi; Gómez-Restrepo, Carlos (2005). "Métodos en investigación cualitativa: triangulación". *Revista colombiana de psiquiatría*, v. 34, n. 1, pp. 118-124.
http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0034-74502005000100008

Peppard, Joe (2007). "The conundrum of IT management". *European journal of information systems*, v. 16, n. 4, pp. 336-345.
https://www.researchgate.net/publication/220393150_The_conundrum_of_IT_management
https://doi.org/10.1057/palgrave.ejis.3000697

Pinto, Roger; **Grawitz, Madeleine** (1967). "Analyse de contenu et theorie". In: Pinto, Roger; Grawitz, Madeleine. *Méthodes des sciences sociales*. Paris: Dalloz, pp. 456-499. ISBN: 978 2247041138

Porter, Michael; **Millar, Victor** (1985). "How information gives you competitive advantage". *Harvard business review*, v. 64, n. 4, p. 149.
https://hbr.org/1985/07/how-information-gives-you-competitive-advantage

Posthumus, Shaun; **Von-Solms, Rossouw** (2004). "A framework for the governance of information security". *Computers & security*, v. 23, n.8, pp. 638-646.
https://doi.org/10.1016/j.cose.2004.10.006

Proctor, Robert W.; **Chen, Jing** (2015). "The role of human factors/ergonomics in the science of security: Decision making and action selection in cyberspace". *Human factors*, v. 57, n. 5, pp. 721-727.
https://doi.org/10.1177/0018720815585906

Puhakainen, Petri; **Siponen, Mikko** (2010). "Improving employees' compliance through information systems security training: an action research study". *MIS quarterly*, v. 34, n. 4, pp. 757-778.
http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2933&context=misq

Rahim, Noor-Hayani-Abd; **Hamid, Suraya**; **Mat-Kiah, Miss-Laiha**; **Shamshirband, Shahaboddin**; **Furnell, Steven** (2015). "A systematic review of approaches to assessing cybersecurity awareness". *Kybernetes*, v. 44, n. 4, pp. 606-622.
https://umexpert.um.edu.my/file/publication/00007217_125724.pdf
https://doi.org/10.1108/K-12-2014-0283

Rantos, Konstantinos; **Fysarakis, Konstantinos**; **Manifavas, Charalampos** (2012). "How effective is your security awareness program? An evaluation methodology". *Information security journal: A global perspective*, v. 21, n. 6, pp. 328-345.
https://goo.gl/3Dxh1R
http://dx.doi.org/10.1080/19393555.2012.747234

Salmela, Hannu (2007). "Analysing business losses caused by information systems risk: a business process analysis approach". *Journal of information technology*, v. 23, n. 3, pp. 185-202.
http://dx.doi.org/10.1057/palgrave.jit.2000122

Sanou, Brahima (2014). *The world in 2014: ICT facts and figures*. Switzerland: ITU World Telecommunication/ICT Indicators database.
http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

Sen, Ravi; **Borle, Sharad** (2015). "Estimating the contextual risk of data breach: An empirical approach". *Journal of management information systems*, v. 32, n. 2, pp. 314–341.
https://doi.org/10.1080/07421222.2015.1063315

Sircar, Sumit; **Choi, Jung** (2009). "A study of the impact of information technology on firm performance: a flexible production function approach". *Information systems journal*, v. 19, n. 3, pp. 313-339.
https://doi.org/10.1111/j.1365-2575.2007.00274.x

Citado por **Doherty, Neil F.**; **Anastasakis, Leonidas**; **Fulford, Heather** (2009). "The information security policy unpacked: a critical study of the content of university policies". *International journal of information management*, v. 29, n. 6, p. 449.
https://doi.org/10.1016/j.ijinfomgt.2009.05.003

Syalim, Amril; **Hori, Yoshiaki**; **Sakurai, Kouichi** (2009). "Comparison of risk analysis methods: *Mehari*, *Magerit*, *NIST800-30* and *Microsoft's security management guide*". In: *Intl conf on availability, reliability and security*, pp. 726. IEEE.
*https://doi.org/*10.1109/ARES.2009.75

Testa, James (2001). "La base de datos del ISI y su proceso de selección de revistas". *Acimed*, v. 9, n. 4, pp. 138-140.
http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352001000400023

Thomson, Kerry-Lynn; **Von-Solms, Rossouw**; **Louw, Lynette** (2006). "Cultivating an organizational information security culture". *Computer fraud & security*, n. 10, pp. 7-11.
https://doi.org/10.1016/S1361-3723(06)70430-4

Tranfield, David; **Denyer, David**; **Smart, Palminder** (2003). "Towards a methodology for developing evidence informed management knowledge by means of systematic review". *British journal of management*, v. 14, n. 3, pp. 207-222.
https://www.cebma.org/wp-content/uploads/Tranfield-et-al-Towards-a-Methodology-for-Developing-Evidence-Informed-Management.pdf
https://doi.org/10.1111/1467-8551.00375

Valentine, J. Andrew (2006). "Enhancing the employee security awareness model". *Computer fraud & security*, n. 6, pp. 17-19.
https://www.researchgate.net/publication/222686702_Enhancing_the_employee_security_awareness_model
https://doi.org/10.1016/S1361-3723(06)70370-0

Von-Solms, Bassie (2000). "Information security. The third wave?". *Computers & security*, v. 19, n. 7, pp. 615-620.
https://www.researchgate.net/publication/220614516_Information_Security_-_The_Third_Wave
https://doi.org/10.1016/S0167-4048(00)07021-8

Von-Solms, Basie (2001). "Information security. A multidimensional discipline". *Computers & security*, v. 20, n. 6, pp. 504-508.
http://docslide.us/documents/information-security-a-multidimensional-discipline.html
https://doi.org/10.1016/S0167-4048(01)00608-3

Von-Solms, Bassie (2006). "Information security. The fourth wave". *Computers & security*, v. 25, n. 3, pp. 165-168.
https://www.researchgate.net/publication/220614702_Information_Security_-_The_Fourth_Wave
https://doi.org/10.1016/j.cose.2006.03.004

Von-Solms, Bassie; **Von-Solms, Russouw** (2004a). "The 10 deadly sins of information security management". *Computers & security*, v. 23, n. 5, pp. 371-376.
https://www.researchgate.net/publication/222432067_The_10_deadly_sins_of_information_Security_management
https://doi.org/10.1016/j.cose.2004.05.002

Von-Solms, Rossouw; **Von-Solms, Bassie** (2004b). "From policies to culture". *Computers & security*, v. 23, n. 4, pp. 275-279.
https://doi.org/10.1016/j.cose.2004.01.013

Von-Solms, Bassie; **Von-Solms, Rossouw** (2005). "From information security to business security?". *Computers & security*, v. 24, n. 4, pp. 271-273.
https://doi.org/10.1016/j.cose.2005.04.004

Vroom, Cheryl; **Von-Solms, Rossouw** (2004). "Towards information security behavioural compliance". *Computers & security*, v. 23, n. 3, pp. 191-198.
https://www.researchgate.net/publication/222358341_Towards_information_security_behavioral_compliance
https://doi.org/10.1016/j.cose.2004.01.012

Wallace, William (2000). "La gestión del conocimiento. William Wallace explica cómo el capital intelectual aumenta la productividad". *La nación*, 15 agosto.
http://www.lanacion.com.ar/183309-la-gestion-de-conocimiento
http://www.a3net.net/es/gescon/definiciones.htm

Wang, Ju-An; **Guo, Minzhe**; **Hao, Wang**; **Zhou, Linfeng** (2012). "Measuring and ranking attacks based on vulnerability analysis". *Information systems and e-business management*, v. 10, n. 4, pp. 455-490.
https://www.researchgate.net/publication/251396570_Measuring_and_ranking_attacks_based_on_vulnerability_analysis
https://doi.org/10.1007/s10257-011-0173-5

Ward, John; **Peppard, Joe** (2002). *Strategic planning for information systems*. 3rd ed. Chichester: Wiley Publishing, pp. 640. ISBN 978 0470841471.

Citado por **Doherty, Neil F.**; **Anastasakis, Leonidas**; **Fulford, Heather** (2009). "The information security policy unpacked: a critical study of the content of university policies". *International journal of information management*, v. 29, n. 6, p. 449.
https://doi.org/10.1016/j.ijinfomgt.2009.05.003

Weirich, Dirk; **Sasse, Martina-Angela** (2005). "Persuasive password security". In: *Procs CHI EA'01 CHI'01 Extended abstracts on human factors in computing systems*. pp. 139-140. ISBN: 1581133405
https://www.researchgate.net/publication/234798659_Persuasive_password_security
https://doi.org/10.1145/634067.634152

Whitman, Michael (2004). "In defense of the realm: understanding threats to information security". *International journal of information management*, v. 24, n. 1, pp. 43-57.
https://www.researchgate.net/publication/222118125_In_defense_of_the_realm_Understanding_threats_to_information_security
https://doi.org/10.1016/j.ijinfomgt.2003.12.003

Whitman, Michael E.; **Townsend, Anthony M.**; **Aalberts, Robert J.** (2001). "Information systems security and the need for policy". In: Dhillon, Gurpreet. *Information security management: Global challenges in the new millennium.* Las Vegas: University of Nevada, p. 10. ISBN: 978 1878289780.
http://dx.doi.org/10.4018/978-1-878289-78-0

Citado por: **Aurigemma, Salvatore**; **Panko, Raymond** (2012). "A composite framework for behavioral compliance with information security policies". In: *45th Hawaii intl conf on system sciences*, pp. 3248-3257. IEEE.
https://goo.gl/I433tj
https://doi.org/10.1109/HICSS.2012.49

Wiant, Terry (2005). "Information security policy's impact on reporting security incidents". *Computers & security*, v. 24, n. 6, pp. 448-459.
https://doi.org/10.1016/j.cose.2005.03.008

Zammuto, Raymond; **Griffith, Terri**; **Majchrzak, Ann**; **Dougherty, Deborah**; **Faraj, Samer** (2007). "Information technology and the changing fabric of organization". *Organization science*, v. 18, n. 5, pp. 749-762.
https://www.academia.edu/14882285/Information_Technology_and_the_Changing_Fabric_of_Organization
https://doi.org/10.1287/orsc.1070.0307

Zhou, Minqi; **Zhang, Rong**; **Xie, Wei**; **Qian, Weining**; **Zhou, Aoying** (2010). "Security and privacy in cloud computing: A survey". In: *SKG'10 Procs of the 2010 6th intl conf on semantics, knowledge and grids*, pp. 105-112. Washington, DC, USA: IEEE.
https://doi.org/10.1109/SKG.2010.19

Zissis, Dimitrios; **Lekkas, Dimitrios** (2012). "Addressing cloud computing security issues". *Future generation computer systems*, v. 28, n. 3, pp. 583-592.
https://www.researchgate.net/publication/220285301_Addressing_cloud_computing_security_issues
https://doi.org/10.1016/j.future.2010.12.006